

APPENDIX A

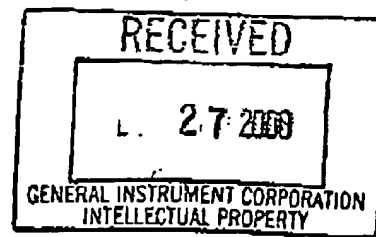
General Instrument Corporation Invention Record Form No. D02635
Inventor: Paul Moroney

General Instrument Corporation®

Intellectual Property Department
For Internal Use Only

Invention Record Form

GI Docket No. 32635



I. Administrative Information

1. Short Descriptive Title of the Invention:

Digital Cinema System Concept

2. Identify all persons who contributed to this invention, including persons from other divisions and/or outside companies:

	Inventor 1	Inventor 2
Full Legal Name	Paul Moroney	
Home Address	3411 Western Springs Road	
City, State, Zip	Olivenhain, CA 92024	
Citizenship	USA	
Division/Co. Location	Motorola BCS, San Diego	
Office Phone No.	858 404 2446	
Mgr.'s Name & Phone No.	Geoff Roman	
Signature of Inventor	<i>Paul Moroney</i>	
Date	12-22-2000	

	Inventor 3	Inventor 4
Full Legal Name		
Home Address		
City, State, Zip		
Citizenship		
Division/Co. Location		
Office Phone No.		
Mgr.'s Name & Phone No.		
Signature of Inventor		
Date		

3. ☐ Check box if there are additional inventors listed on separate sheets. Additional information concerning inventors, if any.

GI CONFIDENTIAL & PROPRIETARY

Rev. 02/98

D2035

Invention Record Form

II. Background Information

1. Do you believe this invention was developed while working under or in the performance of experimental, developmental or research work called for by a government contract or with the understanding that a government contract would be awarded? ☒ No ☐ Yes If yes, please explain:
2. Has your invention been disclosed to anyone outside General Instrument in a speech, exhibit, presentation, product, product manual, report, lecture, trade show, technical article, publication or otherwise? ☒ No ☒ Yes If yes, please explain:
Presented to Dave Baddow of Liberty LiveWire, inside GI facility, April 2000.
3. Is this invention related to any previous GI invention disclosures of which you are aware (made by you or someone else)? ☒ No ☐ Yes If yes, please explain:
4. Name of product(s) and/or project(s) for which this invention was developed:
Developed for Digital Cinema system as concept approach.
5. Planned or actual use of invention:
Hope for use in e-cinema standards and products in future, as field develops
6. What economic benefits do you think GI can derive from this invention?
Possible production of compression and security modules, and possible source side off-line compression and encryption support.
7. When do you expect a product incorporating this invention to be sold, offered for sale or shown to someone outside of GI? (If a product or prototype has already been sold, offered for sale or shown, please identify the earliest date this happened.)
Uncertain
8. Has a working model of the invention been built and tested (or appropriate software been written)?
☒ No ☐ Yes If yes, who has witnessed a demonstration, and when?
9. List below any patents, publications, articles, texts, products, etc. which describe technology similar to your invention including reference material which may be useful in understanding the background technology of your invention. (Use a separate sheet if necessary and attach a copy of each item. Please include copies of all bibliographical information.) (Use a separate sheet if necessary)



Signature of Submitter(s)



Read and understood by [Witness Signature(s)]

12-22-00

Date

12-22-2000

Date

D2635

Invention Record Form

III. Description of the Invention

1. Please provide a very brief (i.e., one short sentence) summary of your invention.

System for supporting digital (electronic) cinema incorporating compression/ decompression and security technology, with module forms for easy upgrade

2. Briefly describe the field of technology to which your invention relates.

3. Briefly describe the problems, issues or needs which led to the invention.

Digital Cinema is an evolving field: it needs an approach that can evolve with technology, yet still provide a secure approach, with high quality.

4. How have others addressed these problems, issues or needs?

Others may build a fixed solution, which is either less secure or needs to be completely replaced as technology progresses.

5. Describe those particular features or functions of your invention which you think may be novel or technical advancements over the technology you listed in section II.9.

Theater side equipment will be built as a module that plugs directly into the theater projector, and locks inside. The module will receive IP packets of MPEG video and audio content, and decrypt them and decompress them inside the module. A watermark specific to the projector is also added inside the module, for maximum security. When the compression techniques improve, you only replace the module, not the entire projector. This module needs to be inside the projector for maximum secure identification of that projector as the location of decryption, decompression, and display. This keeps a pirate from accessing the clear digital content electronically. If the pirate films the displayed movie, the watermark is present for identification. If security algorithms change, again, only the module must be replaced.

6. Best Mode: Describe any and all preferences you personally have regarding how to best implement, build, produce or use your invention (e.g., preferred parts, materials, techniques, etc. which you feel are best in practicing your invention). Each submitter's opinion is important here, even if there is disagreement. Please list anything you think will make the invention better in any way.

The security algorithms and compression approaches must be standards-based, and state of the art. We prefer MPEG-4 for video and audio, RTP for transport over IP networks, either real time or non-real time and stored at the theater servers, and the Advanced Encryption Standard for encryption of the multi-media.

7. Briefly describe any alternative uses, variations or modifications of your invention which you contemplate.

8. Please provide any additional information you think should be known by the attorney reviewing this form.

Use of MPEG-4 is not novel. Use of IP to deliver content is not novel, nor is encrypting that content. It is the combination of the system approach and the module approach that provides value, and the other details described below.

9. Please provide a detailed description of your invention. Your description should ideally provide as many details of your invention as possible in order to achieve optimal patent protection. An ideal disclosure should describe the construction and operation of the invention including drawings (flow charts, schematics, block diagrams, mechanical drawings, photographs, etc.) and any relevant engineering laboratory notebook pages, reports, program listings, etc. If you have already prepared reports or other descriptive information, there is no need to rewrite it. Simply attach it and reference it in your invention disclosure data sheet (for example, "see attached 9 page engineering progress report addressed to John Doe dated 1 Jan., 1992 for description of amplifier circuit").

Please see the attached powerpoint slides dated 11/4/99, 3/2/2000, and 4/26/2000, for prior documentation of the idea flow.

Digital Cinema is an evolving field. The movie studios want an approach that can provide quality.

Paul Sperry
Signature of Submitter(s)

12-22-00
Date

Date

John Doe
Read and understood by [Witness Signature(s)]

12-22-2000
Date

Date

CONFIDENTIAL & PROPRIETARY

Invention Record Form

D2635

security, and low distribution cost. In fact, their primary motivation may be said to be the reduction in distribution costs for digital content as compared to film duplication! However, digital content requires that the theaters install digital servers, and digital electronic projectors, which is quite a cost hit. When you combine the complete change in equipment, with the new distribution approach, and consider the merits of digitally projected content, where quality is excellent for every showing, and the choice of what to project can change for each showing, you have a total industry paradigm shift. Thus the studios are treating this as revolutionary, working with standards groups to redefine everything about the process. They thus want better quality, lower cost, and better security as compared to today's film based approach.

Yet technology is not there with the perfect answer, thus we need an approach that can evolve with technology and time. Since the state of the art in quality and security will change, so must the system.

The studio and movie industry is not enormous. If they redefine all the relevant technology components as new, the costs of system development and product evolution will be enormous. As far as is possible, this industry must exploit existing approaches, approaches developed for other industries and needs. Low cost is also driven by standards, as opposed to proprietary solutions, so the final approach should be very standards based. Only where proprietary approaches provide a special value, or parallel solutions can still work, should they exist. One example is in the key distribution portion of the security approach. Multiple solutions can exist in the same industry. Another example is in the compression technology selected. If a consumer product standard was chosen, then pirates could more easily steal and access useful content. If the format is distinct from that of ordinary consumer electronics, then there is a natural protection based solely on the lack of cheap products to view stolen content!

Our system approach employs security algorithms and compression approaches that are standards-based, and state of the art. We prefer MPEG-4 for video and audio, at bit rates and resolutions that place it beyond the reach of regular consumer electronics devices and PCs. Thus we can use a standard that is proven and known, and still be secure. We prefer the RTP protocol for transport over IP networks, either real time or non-real time, which means that off-the-shelf software can be purchased, or nearly so. Content delivered to most theater serves would be in the form of IP packets, which opens a wide range of today's delivery networks and simultaneously allows the use of off-the-shelf server technology. We prefer the use of triple DES and/or the Advanced Encryption Standard for encryption of the multi-media. These standards are withstood the test of time, and thus encrypted packets delivered over IP networks will be well protected.

Theater side system design will be based upon the key premise that the decryption of valuable content must be placed as close to the ultimate consumer point of "consumption" as possible, to reduce piracy opportunities and also to leave ultimate control in the hands of the owners of the material, the studios. Thus a theater owner cannot decrypt content on his own; the equipment itself must be provisioned by the owner to do so. To place the vital decryption process as close to the viewing point as possible, it should be placed inside the very expensive digital projector itself, which sits in each theater projection room. If decryption occurs in the projector, so must decompression, and thus the interface of decrypted decompressed high quality video to the projection "guns" or silicon mirrors or LCD light valves or whichever projection technology is employed. Projector specific watermarking will occur in the same location, for the ultimate in confidence that the watermarked viewed movie was viewed in the exact theater where the projector is mounted. A GPS circuit can even be embedded in the projector for increased confidence that the projector physical location is known.

Unfortunately, projector technology is not yet at the ultimate in-viewing desired. Some feel that today's projectors cannot achieve the quality delivered by a movie film copy that is properly shot and not yet worn down by repeated playing. Thus we know that the projectors will change for some time to come. As projector video quality and resolution improve with time, so must the resolution delivered to that projector. Today's compression and decompression hardware will also evolve to provide better and better quality and resolution. Today's decryption and watermarking and key management will also evolve

Paul J. ...
Signature of Submitter(s)

12-22-00
Date

John V. ...
Read and understood by [Witness Signature(s)]

12/22/2000
Date

Invention Record Form

D2635

to provide better watermarks, more secure key management, and faster or more secure decryption.

These three evolutions may be parallel, or they may differ. In either case, we need a way to decouple them so that each technology can improve on its own. A theater owner should be able to upgrade the projector without upgrading all the security and decompression and watermarking and key management. Cost-wise, these divide nicely between the projector and everything else.

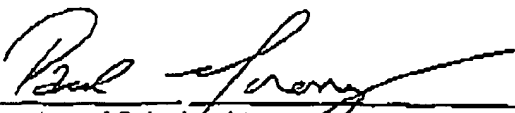
Thus I propose that the decryption, decompression, key management, and watermarking be built as a single hardware/software module, which is replaceable in the theater. [Projectors are large and too valuable to send to a factory to upgrade the module.] The module must be self-contained, surrounded by a secure envelope for tamper protection and identification, and locked inside the projector body via a physically secure approach, such as a key. For further security, the module should have a connection path to the IP network, so that it can inform the content owner of any attempts to remove it or tamper with it. A variety of techniques are possible, including power loss detection, and automatic reporting, so that if the unit is cut off from the content owners or the key management system, silence is interpreted as a violation.

With such an approach, all the usual forms of secure access can be provided; subscription access, pay-per-view access, store and forward access, and the key management system can operate in a broadcast mode where reportback is infrequent, or a full IP network two way mode, where continuous communication with the key management system is present.

The module will receive IP packets of MPEG video and audio content, and decrypt them and decompress them inside the module. The module will receive key management messages from the key management center(s), and process them for proper access to content. A watermark specific to the projector is also added inside the module, for maximum security. A watermark provided by the content owner can also be processed and evaluated for the conditions under which the content may be decrypted [viewed]. The combination of the module being tamper-resistant, and located locked within the projector, keeps a pirate from accessing the clear digital content electronically. If any pirate films the displayed movie, with a portable camera, as is common today, the watermark is present for identification of the exact theater from which the theft occurred.

Note that if projector manufacturers cannot be prevailed upon to provide a location and power for such a module, the concept still has value. To achieve the same goals, the module would need to be after-market mounted either under or along side the projector, physically mounted to it. The clear analog or digital video interfaces to the projector must be buried through the mounting process, as that interface carries the signals that represent the clear content. If this cannot be achieved for any reason, there is still value. By placing the decryption, decompression, and watermarking all together in a secure tamper resistant module/unit, the content owner at last has the confidence that

1. A pirate has access to only very high rate digital content at the interface, making the job of recording it very challenging, and
2. If recorded and stolen in digital form, the watermark is present, and
3. Modular upgrade is easy for the theater


Signature of Submitter(s)


Read and understood by [Witness Signature(s)]

12-22-2006
Date

12-22-2006
Date

GI CONFIDENTIAL & PROPRIETARY

Rev 02/98

D2635

Advanced Technology Update

November 4, 1999

Paul Moroney

© General Instrument

D-Cinema

◆ Keys:

- studio relationship and control
- standards
- projection
- compression
- security

- ◆ GI would supply compression and security technology to a consortium [funded], with probable partial ownership

© General Instrument

D2635

Source Coding

- ◆ General thrust away from consumer technologies
- ◆ No one answer; must evolve, and not be limited by the projector
- ◆ Systems must incorporate real-time when needed
- ◆ Off-line encoding typical for films

© General Instrument

Company Confidential

GI Proposal

- ◆ Standards focus through MPEG-2 and MPEG-4
- ◆ Extend quality beyond ATSC HD.
- ◆ Ex: 1920 by 1080 60 P could be base film compression, and 50 Mbps minimum, with 1080i reserved for real-time encoding. Higher quality modes would be defined as well, for future proofing.
- ◆ VBR compression

© General Instrument

Company Confidential

GI Proposal

- ◆ Compressed film distribution via satellite, fiber, etc as standard file transfer, TCP/IP, or as multicast UDP.
- ◆ Note: 50 Mbps, 2 hour film = 45 GB storage
- ◆ Server array at theater.
- ◆ Decompression at projector.

© General Instrument

Security Requirements

- ◆ Content Encryption
 - Content encryption prevents the content from being used by anyone not possessing a valid key.
 - Content "ideally" is only decrypted at the final destination
 - An operationally practical, yet highly secure, key management must be employed.

© General Instrument

D2635

Security Requirements

◆ Watermarking

- Persistent protection, as in SDMI
- Protects the content by applying a non-removable, non-forgable mark.
- Ideally, legitimate additions to the watermark trace the content through the entire path to consumer
- Attempts to remove or alter the watermark result in the content quality being degraded beyond usability.

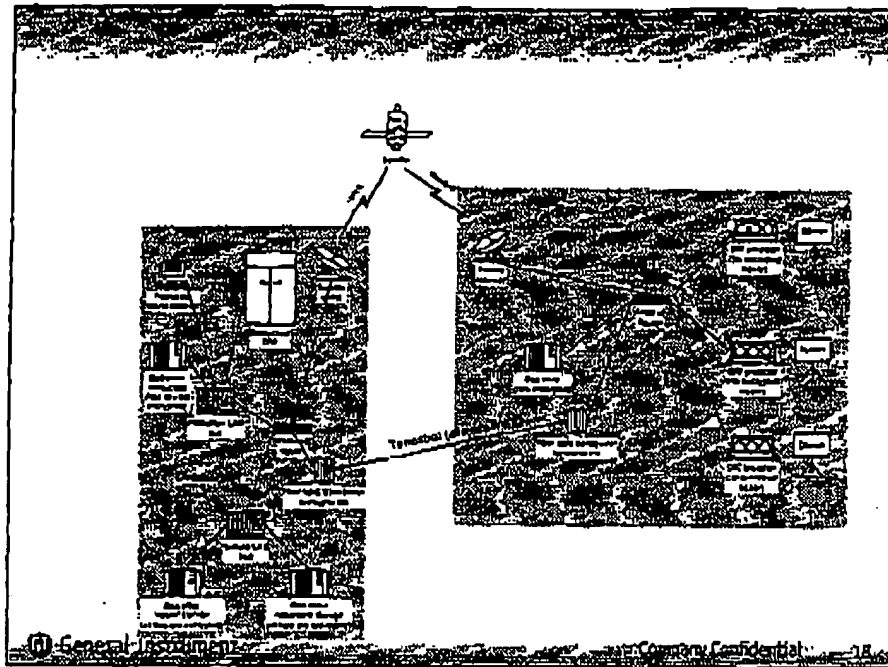
© General Instrument

GI Security proposal

- ◆ Encryption at source, decryption in projector
- ◆ Theater file server storage thus encrypted.
- ◆ Playback control by theater, but decryption control by studio.
- ◆ Source watermark to label content
- ◆ Projector watermark to identify playout
- ◆ Physically protected hardware in projector from GI

© General Instrument

D2635



Decryption Secure Container

- ◆ The objective requirements of the security container is to "protect the content when it is in a form that is easily stolen and easily transported".
- ◆ Projector watermarking must be performed in a secure container.
- ◆ Decryption and decompression must be performed in the "same secure container".
- ◆ Secure container must meet similar security requirements to FIPS 140 level 4.

General Instrument

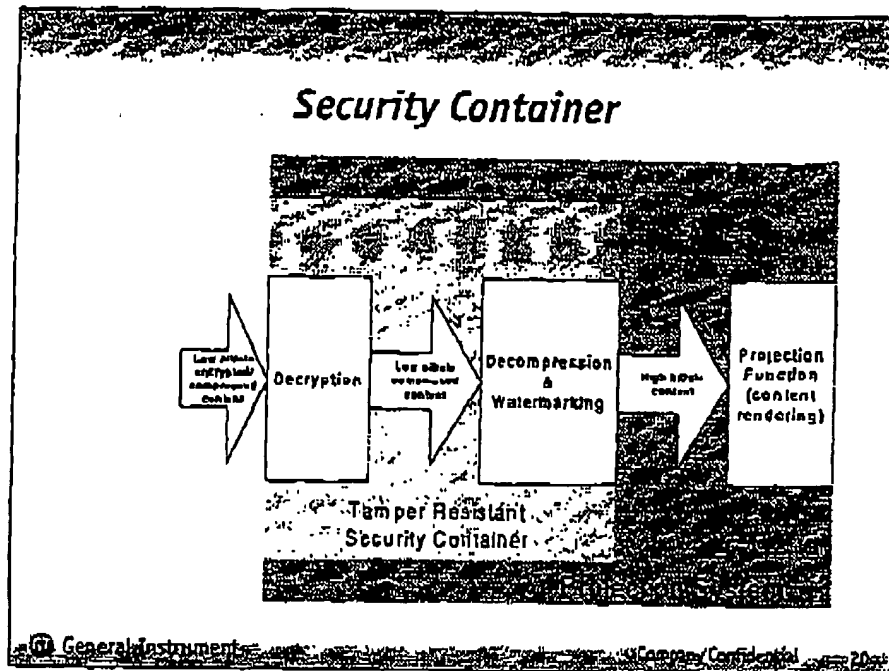
Confidential

Paul Spring 12/22/00

Pete Peterkin

12/22/2000

82635



Agenda

March Engineering Forum

- DNS Programs
- SBNS
- AT:
- lunch
- IPNS
- TNS
- ANS

**MOTOROLA**

Broadband Communications Sector

Advanced Technology Overview

Paul Moroney

3/2/00

**MOTOROLA**

Broadband Communications Sector

Paul Moroney 12-22-00

82635

D-Cinema

- Keys:
 - studio relationship and control
 - standards
 - projection
 - compression
 - security
- GI would supply compression and security technology to a consortium [funded]

**MOTOROLA**

Broadband Communications Sector

GI Proposal

- Compressed film distribution via satellite, fiber, etc as standard file transfer, TCP/IP, or as multicast UDP.
- Note: 50 Mbps, 2 hour film = 45 GB storage
- Server array at theater.
- Decompression at projector.

**MOTOROLA**

Broadband Communications Sector

GI Security proposal

- Encryption at source, decryption in projector
- Theater file server storage thus encrypted.
- Playback control by theater, but decryption control by studio.
- Source watermark to label content
- Projector watermark to identify playout
- Physically protected hardware in projector from GI

**MOTOROLA**

Broadband Communications Sector

*Beafay 12.22.06**Feb 12/22/2006*

DeW

BLANK PAGE

Digital Cinema Directions

Paul Moroney

4/26/2000

AEREC-1ST

D-Cinema

■ Keys:

- studio relationship and control
- standards [SMPTE, MPEG-4]
- projection
- compression
- security

- Motorola to supply compression and security technology to a consortium, & drive/participate in standards process [funded]

AEREC-1ST

Paul Moroney 12-22-00

Source Coding

- General thrust away from consumer technologies
- No one answer; must evolve, and not be limited by the projector
- Systems must incorporate real-time when needed
- Off-line encoding typical for films

ALBECAST

Motorola Strawman

- Standards focus past MPEG-2 to MPEG-4
- Extend quality beyond ATSC HD.
 - Ex: 1920 by 1080 24 P (60 P) could be base film compression, and 50 Mbps minimum, with 1080i reserved for real-time encoding. Higher quality modes would be defined, same compression technology for evolution.
- VBR compression, leverage investment & expertise in high quality SD and HD compression

ALBECAST

Dale SS

Motorola Strawman

- Compressed film distribution via satellite, fiber, etc as standard file transfer, TCP/IP, or as multicast UDP.
- Note: 50 Mbps, 2 hour film = 45 GB storage
- Server array at theater.
- Decompression at projector.

AERCAST

Security Requirements

- Content Encryption
 - Content encryption prevents the content from being used by anyone not possessing a valid key.
 - Content "ideally" is only decrypted at the final destination
 - An operationally practical, yet highly secure, key management must be employed.

AERCAST

Paul Fung 12-22-05

J. J. Fung 12/22/2005

D2635

Security Requirements

■ Watermarking

- Persistent protection, as in SDMI
- Protects the content by applying a non-removable, non-forgable mark.
- Ideally, legitimate additions to the watermark trace the content through the entire path to consumer
- Attempts to remove or alter the watermark result in the content quality being degraded beyond usability.
- Efficient and robust, given compression choice

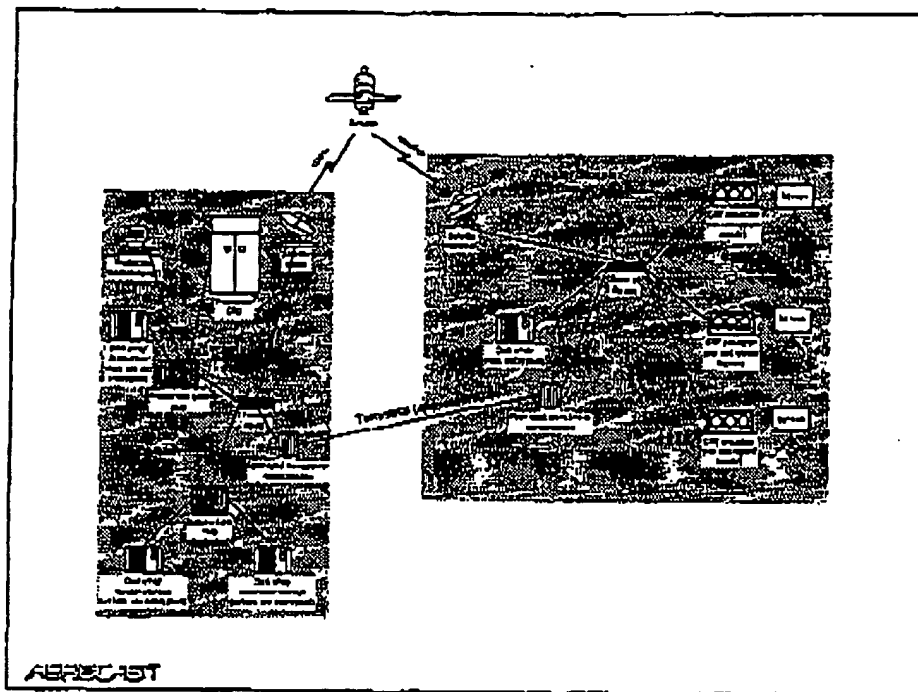
ASRECAST

Motorola Security Strawman

- Encryption at source, decryption in projector
- Theater file server storage thus encrypted.
- Playback control by theater, but decryption control by studio.
- Source watermark to label content
- Projector watermark (fingerprint) to identify playout
- Physically protected hardware in projector from GI

ASRECAST

02635



Decryption Secure Container

- Requirement of the security container is to "protect the content when it is in a form that is easily stolen and easily transported".
- Projector watermarking must be performed in a secure container.
- Decryption and decompression must be performed in the "same secure container".
- Secure container must meet similar security requirements to FIPS 140 level 3 or 4.

AEREC-15T

Benefury 12-22-00

D2635

